CLAIMS:

1. A secure communication system including a source device and at least one sink device; information being transferred from the source device to the sink device in a communication session including the transfer of a plurality of packets from the source device to the sink device; each packet including a data field for transferring a portion of the information;

the source device including:

a key generator for, at the initiative of the source device, generating an active source session key in a predetermined sequence of source session keys **Ksource**$_\mathbf{i}$;

an encryptor for encrypting at least part of the data field of a packet under control of the active source session key; the encrypted part of the data field including a sub-field designated as a key check block field;

the sink device including:

a key generator for generating a plurality of candidate sink session key in a predetermined sequence of sink session keys **Ksink**$_\mathrm{i}$, where for each index **i** in the sequence the respective sink session key **Ksink**$_\mathbf{i}$ corresponds to the respective source session key **Ksource**$_\mathbf{i}$;

a decryptor for decrypting at least part of the data field of a received packet under control of a sink session key;

a key resolver operative to determine which of the candidate sink session keys corresponds to the source session key used to encrypt the encrypted part of a received packet, by causing the decryptor to decrypt the data in the key check block field of the received packet under control of each time a different one of the plurality of candidate sink session keys until a valid decryption result is found; and to cause the decryptor to decrypt a remaining encrypted part of the data field of the packet under control of the candidate sink session key which produced the valid decryption result.

2. A secure communication system as claimed in claim 1, wherein the plain-text form of the key check block in the key check block field is a public data block.

3. A secure communication system as claimed in claim 1, wherein the plain-text form of the key check block in the key check block field is a data block agreed between the source and sink device before starting the transfer of the information and used for the entire communication session.

4. A secure communication system as claimed in claim 1, wherein the plain-text form of the key check block in the key check block field changes at least once during the communication session.

5. A secure communication system as claimed in claim 4, wherein the source and sink device include corresponding key check block generators for generating the plain-text form of the key check block and effecting the change of the plain-text form of the key check block.

6. A secure communication system as claimed in claim 4, wherein the plain-text form of the key check block of a particular packet is derived from information transferred in a packet preceding the particular packet.

7. A secure communication system as claimed in claim 6, wherein the plain-text form of the key check block is derived from information transferred in a packet immediately preceding the particular packet.

8. A secure communication system as claimed in claim 6 or 7, wherein the plain-text form of the key check block of a particular packet is identical to the plain-text form of a predetermined data block, other than the key check block, in an encrypted part of the data field of a packet preceding the particular packet.

9. A sink device for use in a secure communication system wherein a source device autonomously can change a source session key used for encrypting at least part of the data field of a packet transferred from the source device to the sink device; the encrypted part of the data field including a sub-field designated as a key check block field;
the sink device including:

a key generator for generating a plurality of candidate sink session key in a predetermined sequence of sink session keys **Ksink**$_i$, where for each index **i** in the sequence the respective sink session key **Ksink$_i$** corresponds to the respective source session key **Ksource$_i$**;

a decryptor for decrypting at least part of the data field of a received packet under control of a sink session key;

a key resolver operative to determine which of the candidate sink session keys corresponds to the source session key used to encrypt the encrypted part of a received packet, by causing the decryptor to decrypt the data in the key check block field of the received packet under control of each time a different one of the plurality of candidate sink session keys until a valid decryption result is found; and to cause the decryptor to decrypt a remaining encrypted part of the data field of the packet under control of the candidate sink session key which produced the valid decryption result.

10. A method of secure communication between a source device and at least one sink device; information being transferred from the source device to the sink device in a communication session including the transfer of a plurality of packets from the source device to the sink device; each packet including a data field for transferring a portion of the information; the method including:

at the initiative of the source device generating an active source session key in a predetermined sequence of source session keys **Ksource$_i$**;

encrypting at least part of the data field of a packet under control of the active source session key; the encrypted part of the data field including a sub-field designated as a key check block field;

transferring the packet from the source device to the sink device;

generating a plurality of candidate sink session key in a predetermined sequence of sink session keys **Ksink$_i$**, where for each index **i** in the sequence the respective sink session key **Ksink$_i$** corresponds to the respective source session key **Ksource$_i$**;

determining which of the candidate sink session keys corresponds to the source session key used to encrypt the encrypted part of a received packet, by decrypting the data in the key check block field of the received packet under control of each time a different one of the plurality of candidate sink session keys until a valid decryption result is found; and

decrypting a remaining encrypted part of the data field of the packet under control of the candidate sink session key which produced the valid decryption result.

11. A method of in a sink device in a secure communication system detecting a change of a session key effected by a source device in the system; information being transferred from the source device to the sink device in a communication session including the transfer of a plurality of packets from the source device to the sink device; each packet including a data field for transferring a portion of the information; at least part of the data field of a packet being encrypted under control of an active source session key in a predetermined sequence of source session keys **Ksource**$_i$; the encrypted part of the data field including a sub-field designated as a key check block field; the method including:

generating a plurality of candidate sink session key in a predetermined sequence of sink session keys **Ksink**$_i$, where for each index **i** in the sequence the respective sink session key **Ksink**$_i$ corresponds to the respective source session key **Ksource**$_i$;

determining which of the candidate sink session keys corresponds to the source session key used to encrypt the encrypted part of a received packet, by decrypting the data in the key check block field of the received packet under control of each time a different one of the plurality of candidate sink session keys until a valid decryption result is found; and

decrypting a remaining encrypted part of the data field of the packet under control of the candidate sink session key which produced the valid decryption result.

12. A computer program product where the program product is operative to cause a computer to perform the method of claim 11.